[4910-62-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

[Docket No. TSA-2004-19160]

Notice of Final Order for Secure Flight Test Phase; Response to Public Comments on Proposed Order and Secure Flight Test Records

AGENCY: Transportation Security Administration (TSA), Department of Homeland Security (DHS).

ACTION: Notice.

SUMMARY: This notice responds to public comments received in response to three documents that the Transportation Security Administration (TSA) published in the Federal Register on September 24, 2004, related to testing of a new domestic passenger prescreening program known as Secure Flight. Secure Flight is an aviation passenger prescreening program that, once operational, would identify passengers known or reasonably suspected to be engaged in terrorist activity in order to allow action to be taken to prevent them from boarding a domestic flight or to ensure that appropriate additional security screening procedures are applied. Under the program, TSA would compare passenger reservation information for domestic flights, primarily in the form of passenger name records (PNRs), to information maintained by the Federal Government about individuals known or reasonably suspected to be engaged in terrorist activity.

In preparation for testing the feasibility of the Secure Flight program, on September 24, 2004, TSA issued a Federal Register notice establishing a system of records under the Privacy Act for purposes of the Secure Flight program during the test

phase. TSA also published a notice in the Federal Register that the agency had submitted to the Office of Management and Budget (OMB) a request for approval to collect PNRs from aircraft operators to test the Secure Flight program. That notice included the text of a proposed order to certain aircraft operators directing them to provide a limited set of historical PNRs to TSA. OMB subsequently has approved the information collection through March 31, 2005, and assigned OMB control number 1652-0025. In addition, TSA published a Privacy Impact Assessment for the testing phase of the Secure Flight program.

This Federal Register notice that TSA publishes today addresses public comments received in response to the Federal Register notices published on September 24, 2004, and describes changes made to TSA's proposed order, which TSA now is issuing in final form.

FOR FURTHER INFORMATION CONTACT: Lisa Dean, Privacy Officer, Transportation Security Administration, 601 South 12th Street, Arlington, VA 22202-4220; telephone (571) 227-3947; facsimile (571) 227-2594; e-mail lisa.dean@dhs.gov.

SUPPLEMENTARY INFORMATION:

Background

On September 24, 2004, TSA published in the Federal Register three notices related to TSA's plan to issue a final order to aircraft operators in order to obtain PNRs for testing of a new domestic passenger prescreening program know as Secure Flight (69 FR 57342, 57345, and 57352). This Federal Register notice that TSA is publishing today responds to public comments received in response to the notices published on September

24, 2004, and provides public notice of the final order that TSA is issuing for purposes of testing the Secure Flight program.

Secure Flight Program

The Secure Flight program is an effort to move the existing passenger prescreening process into the Federal Government in order to make the process more effective, consistent, and efficient for the traveling public. By administering this screening process within the Federal Government, the Secure Flight program will allow for better protection of government watchlist information that currently is provided to aircraft operators.

Secure Flight will involve the comparison of information in PNRs from domestic flights to names in the Terrorist Screening Database (TSDB) maintained by the Terrorist Screening Center (TSC), including the expanded TSA No-Fly and Selectee Lists, in order to identify individuals known or reasonably suspected to be engaged in terrorist activity. TSA anticipates that it will also apply, within the Secure Flight system, a streamlined version of the existing passenger prescreening process, known as the Computer Assisted Passenger Prescreening System (CAPPS), which evaluates information in PNRs that passengers otherwise provide to aircraft operators in the normal course of business.

Simple comparisons of PNR information against records maintained in the TSDB will not permit TSA to identify information provided by passengers that is incorrect or inaccurate, potentially rendering the comparisons less effective. Therefore, on a very limited basis, in addition to testing TSA's ability to compare passenger information with data maintained by TSC, TSA will separately test the use of commercial data to determine if use of such data is effective in identifying passenger information that is

incorrect or inaccurate and reducing the number of false positive matches of passenger information against TSDB records. This test will involve commercial data aggregators whose procedures will be governed by strict privacy and data security protections. TSA will not receive the commercially available data that would be used by commercial data aggregators. TSA will use this test of commercial data to determine whether such use: (1) could identify when passengers' information is inaccurate or incorrect and/or assist with the resolution of false positive matches; (2) would result in inappropriate differences in treatment of any protected category of persons; and (3) could be governed by data security safeguards and privacy protections that are sufficiently robust to ensure that commercial entities or other unauthorized entities do not gain access to passengers' personal information and to ensure that the government does not gain inappropriate access to commercial information about individuals. TSA will defer any decision of whether commercial data will be used in its prescreening programs, such as Secure Flight, until a thorough assessment of test results is completed. If TSA decides to use commercial data for Secure Flight, it will not do so until the agency publishes a new System of Records Notice announcing how commercial data will be used and individuals' privacy will be protected.

TSA's efforts to develop and test the Secure Flight program are fully consistent with the recommendation in the final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), which states at page 392:

> "[I]mproved use of "no-fly" and "automatic selectee" lists should not be delayed while the argument about a successor to CAPPS continues. This screening function should be performed by TSA and it should utilize the larger set of watch lists maintained by the Federal Government. Air carriers should be required to supply the information needed to test and implement this new system."

The expansion of these watchlists to include information not previously included for security reasons will be possible as integration and consolidation of the information related to individuals known or suspected to be engaged in terrorist activity maintained by TSC is completed and the U.S. Government assumes the responsibility for administering the watchlist comparisons. Secure Flight will automate the vast majority of watchlist comparisons, will allow TSA to apply more consistent procedures where automated resolution of potential matches is not possible, and will allow for more consistent response procedures at airports for those passengers identified as potential matches.

Secure Flight represents a significant step in securing domestic air travel and safeguarding terrorism-related national security information, namely, the watchlists. It will dramatically improve consistency and effectiveness of comparisons of passenger information with data now maintained by TSC and will reduce the long-term costs to air carriers and passengers associated with maintaining the present system, which is operated individually by each aircraft operator that flies in the United States.

Prior Federal Register Notices

In order to test the feasibility of the Secure Flight program, TSA must obtain a sample of passenger information for domestic flights. In preparation for obtaining this information for testing purposes, on September 24, 2004, TSA published three public notices in the Federal Register. First, TSA published a system of records notice in accordance with the Privacy Act of 1974 (5 U.S.C. 552a), including a list of the proposed routine uses of information in the system of records. (69 FR 57345). The system of records notice establishes a new system entitled "Secure Flight Test Records" (hereafter

referred to as DHS/TSA 017), which will govern the collection, maintenance, use, and disclosure of PNRs and other information obtained by TSA for purposes of testing the Secure Flight program. TSA requested public comment on the routine uses for DHS/TSA 017 during a 30-day comment period ending on October 25, 2004.

Second, TSA published in the Federal Register a notice that TSA had submitted to the Office of Management and Budget in accordance with the Paperwork Reduction Act (PRA) of 1995 (44 U.S.C. 3501, et seq.) a request for emergency processing of OMB's review and approval for TSA to collect PNRs from aircraft operators to test the Secure Flight program (PRA notice). (69 FR 57342). That notice included the text of a proposed order to certain aircraft operators directing them to provide a limited set of historical PNRs to TSA that cover commercial scheduled domestic flights. Specifically, the proposed order covered PNRs with domestic flight segments flown during the month of June 2004 and excluded those PNRs with flight segments that occurred after June 30, 2004. The purpose of this limitation was to ensure that during the test phase, TSA does not obtain any information about future travel plans of passengers on domestic flights. The order also proposed to exclude PNR flight segments to or from the U.S. Although not required to do so, TSA requested public comment on the proposed order during a 30-day comment period ending on October 25, 2004. OMB subsequently has approved the information collection through March 31, 2005, and assigned OMB control number 1652-0025.

Third, TSA published in the Federal Register a Privacy Impact Assessment for the test phase of the Secure Flight program, which TSA prepared in accordance with the E-Government Act of 2002. (69 FR 57352).

TSA received approximately 500 public comments on the Privacy Act system of records notice for DHS/TSA 017. Identical versions of most of those comments also were sent to OMB in response to TSA's PRA notice. TSA has reviewed and considered the issues raised by the public comments submitted to TSA and OMB. This notice addresses those issues and describes changes made to TSA's proposed order to aircraft operators, which, after carefully considering the comments, TSA now is issuing in final form.

Public Comments

Public comments on the Secure Flight system of records notice and PRA notice generally focused on one or more of the following categories of issues: (1) the program's effect on individual privacy and civil liberties; (2) the routine uses established for the Secure Flight Test Records System (DHS/TSA 017); (3) passenger consent to the use of historical PNRs; (4) the absence of a redress process; (5) concerns with the use of commercial data; (6) the efficacy of the Secure Flight program; (7) TSA's compliance with the Privacy Act, the PRA, and other laws; and (8) possible conflicts of laws involving European Union (EU) data privacy requirements.

Effect on Individual Privacy and Civil Liberties

A large majority of the commenters viewed the use of PNRs to prescreen passengers against government watchlists as an invasion of privacy and an infringement on their civil liberties, including individuals' right to travel and exercise other Constitutional rights that might be related to travel, such as the freedom of assembly. The National Business Travel Association (NBTA), stated that TSA should balance the need to establish better security measures with policies and procedures that protect civil

liberties and privacy. The NBTA also stated that TSA should not impose unnecessary costs on business travelers.

TSA is aware of, and sensitive to, the need to preserve Americans' freedoms while pursing better security. In implementing a new security measure that affects these interests, it is necessary to move deliberately and cautiously. It is for this very reason that TSA is testing the Secure Flight program before moving forward with an operational system.

The prescreening of passengers against Government watchlists is a security measure that has been in place for several years, performed by aircraft operators, using watchlists provided by the Federal Government. Because the airlines have varying systems by which they implement passenger prescreening, the effectiveness, efficiency, and consistency in response for airline passengers of the current system is limited. The Secure Flight program is an effort to move this prescreening process into the Federal Government in order to make the process more effective, consistent, and efficient for the traveling public. This effort is consistent with a specific aviation security recommendation of the 9/11 Commission.

The Secure Flight program will not impose an unconstitutional burden on an individual's right to travel or exercise other Constitutional rights. The Secure Flight program is a limited, reasonable security screening measure designed to further the Federal Government's compelling interest in protecting aviation security. Except in cases where a passenger may authorize TSA to retain information about him or her for purposes of redress, TSA has no long-term need to retain the information and is seeking approval from the National Archives and Records Administration (NARA) to destroy

passenger information shortly after completion of the passenger's itinerary. Similarly, for purposes of the test phase of the program, TSA is seeking NARA approval to destroy PNRs used for the test after the test has been completed and the results have been evaluated. TSA's purpose in obtaining PNRs is to test the program, not to maintain information on individuals' travel.

TSA agrees with NBTA's comments regarding the need to have policies and procedures that protect passengers' civil liberties and privacy interests and to ensure the Secure Flight program is effective. TSA is in the process of developing redress procedures that will accomplish these goals, as discussed further below.

The Electronic Privacy Information Center (EPIC) objected to TSA's statement in the System of Records notice that the records created and maintained in the course of the Secure Flight test phase should be exempt from a number of the provisions of the Privacy Act, such as the provision allowing individuals to obtain access to certain records containing information about them.

The Privacy Act specifically permits agencies to exempt from certain of its provisions investigatory materials compiled for law enforcement purposes, because allowing individuals access to law enforcement files could impair investigations, particularly those involving complex or continuing patterns of behavior. The intent of the exemption is to prevent access to law enforcement records if that access would alert subjects that their activities are being scrutinized and allow them to take countermeasures to escape detection and prosecution.

In the Secure Flight system of records notice section entitled "Exemptions Claimed for the System", TSA stated that for portions of the system it would invoke

exemptions to the Privacy Act's requirements such as those that: (1) permit individuals to obtain access to, and amend, information pertaining to them; and (2) require that information collected by the agency be relevant and necessary to the agency's statutory purpose. (69 FR 57348). TSA is in the process of preparing a notice of proposed rulemaking to implement these exemptions, which will include a detailed explanation of the basis for invoking the exemptions and will offer the public an opportunity to comment further.

At this point, it is unclear whether TSA will need to invoke these exemptions for the Secure Flight program in its operational stage. In order, however, to preserve its ability to protect classified and law enforcement investigatory information from public disclosure, TSA identified these exemptions in the system of records notice as exemptions it may invoke, if necessary. EPIC noted in its comment that certain information in the system of records, such as PNRs, may not be subject to the exemptions and therefore should be releasable to the affected individual under the Privacy Act. TSA agrees with this view. As stated in the system of records notice, TSA will give individuals access to records in the system pertaining to them to the greatest extent feasible, consistent with law enforcement and national security concerns. It should become clearer during the test phase whether the records in the system may be structured in such a way as to exclude any information that must be withheld from the public for the reasons discussed above.

With regard to the requirement that information collected by the agency be "relevant and necessary," one of the objectives of the test phase is to confirm what information in a PNR is relevant and necessary to conduct an effective comparison of

PNRs to information in the TSDB. The results of the test phase should enable TSA to determine more precisely what passenger information is relevant and necessary to the operation of the Secure Flight program and to limit its collection accordingly during the operational stage.

A number of commenters expressed concern that the Secure Flight program could easily be expanded in the future beyond the scope outlined for the test phase. A number of other commenters anticipated that TSA would use passenger data to monitor where individuals travel and with whom they travel or whether they engage in other activities that could come within the First Amendment protection of freedom of assembly. These commenters have misconstrued the purpose of Secure Flight and the requirements that TSA has proposed for this test.

TSA will neither use passenger information to monitor individuals' movements within the country nor share such information with other agencies or third parties. In fact, for the operational phase of Secure Flight, TSA intends to seek approval from NARA to destroy passenger information shortly after completion of the passenger's itinerary. This will preclude TSA from keeping any record of passenger movements around the country. TSA will not monitor the individuals with whom a particular passenger travels.

If testing of the program indicates that it is a feasible and effective security measure, TSA will initiate a public rulemaking process in which it will provide an appropriate proposal for the workings of the system, as well as the redress process. This process, in conjunction with future publication of a Privacy Act system of records notice for the operational stage of the program will limit TSA's activities under Secure Flight to

those outlined in the notice and serve as the basis for the operation of the program. To the extent that there are any substantial changes to collection of use of information under the program, these will be subject to additional notice and opportunity for public comment. This transparency will serve to prevent so-called "mission creep."

One commenter asked whether Secure Flight would use race, color, gender, age, religion, national origin, political views, origin of a passenger's name, disability, or other personal characteristics as the basis for screening decisions. One commenter suggested that TSA would use gun ownership as a basis for screening decisions. Several commenters stated that TSA should use ethnicity or national origin as a screening factor.

With regard to the use of race, gender, national origin, or other factors listed above, Secure Flight will comply with the Constitution and other applicable law. TSA has adopted and complies with the "Guidance Regarding Use of Race by Federal Law Enforcement Agencies" issued by the United States Department of Justice in June 2003.

Routine Uses

TSA received several comments on TSA's possible disclosure of personal data obtained for testing the Secure Flight program. Under the Privacy Act, TSA is required to list routine uses of the information it will maintain in the system of records created for testing the Secure Flight program. A routine use is a disclosure of a record outside the Department of Homeland Security for a purpose that is compatible with the purpose for which the information was collected. In its system of records notice for DHS/TSA 017, TSA listed the following routine uses for Secure Flight Test Records:

(1) To the Federal Bureau of Investigation where TSA becomes aware of information that may be related to an individual identified in the Terrorist Screening Database as known or reasonably suspected to be or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism;

(2) To contractors, grantees, experts, consultants, or other like persons when necessary to perform a function or service related to the Secure Flight program or the system of records for which they have been engaged. Such recipients are required to comply with the Privacy Act, 5 U.S.C. 552a, as amended;

(3) To the Department of Justice (DOJ) or other Federal agency in the review, settlement, defense, and prosecution of claims, complaints, and lawsuits involving matters over which TSA exercises jurisdiction or when conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) TSA; or (b) any employee of TSA in his/her official capacity; or (c) any employee of TSA in his/her individual capacity, where DOJ or TSA has agreed to represent the employee; or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and TSA determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which TSA collected the records;

(4) To the National Archives and Records Administration (NARA) or other Federal agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906;

(5) To a Congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual; and

(6) To an agency, organization, or individual for the purposes of performing authorized audit or oversight operations.

Some commenters objected to the disclosure of information to other agencies whose missions are unrelated to counterterrorism or security and to foreign governments. TSA has established a very limited set of routine uses for the Secure Flight Test Records. Consistent with the commenters' view, TSA will disclose information to the FBI in connection with its counterterrorism function where TSA becomes aware of information that may be related to an individual identified in the TSDB as known or reasonably suspected to be or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism. The other routine uses applicable to DHS/TSA 017 are necessary for the operation of the agency or the operation and oversight of the Secure Flight program. TSA will not provide any of the information related to the Secure Flight program to foreign governments.

One commenter expressed concern with TSA's plan to allow government contractors access to personal data and suggested that TSA ensure that strong contractual requirements are in place to deter weak data handling practices. TSA will put such contractual requirements in place.

One commenter stated that TSA should ensure that if Secure Flight is used to screen actual passengers, any underlying information about the passenger used to make screening decisions should not be provided to the airlines or screeners.

TSA agrees with this comment. One of the main purposes of Secure Flight is to bring within the Federal Government the watchlist comparison results that currently are in the hands of airlines.

Passenger Consent

Many commenters objected to the government's collection of PNRs for testing purposes because they had not given consent to the collection. As discussed previously, aircraft operators currently use the information in PNRs to conduct passenger prescreening, including watchlists checks and the application of CAPPS. The existence of these prescreening measures has been public knowledge for many years. Therefore, when passengers provide information to aircraft operators in order to purchase air transportation, they have notice that their information will be used for prescreening purposes. In fact, the PNRs TSA will receive for testing Secure Flight already were already used for airline-implemented prescreening in June 2004. Therefore, TSA's collection of the PNRs is consistent with the purposes for which the information in those PNRs originally was collected, and passengers who traveled by air in June 2004 had notice of those purposes.

Redress Process

Commenters noted that TSA has not yet established detailed redress procedures to handle cases where passengers believe they have been unfairly or inaccurately singled out for additional scrutiny as a result of the comparison of their PNRs to information in the TSDB. NBTA stated that TSA should develop a redress process to address inaccuracies

in the databases TSA uses to prescreen passengers, including special procedures for corporate travelers to allow them to continue to fly while any security issue is resolved.

TSA is in the process of developing a robust redress program and has begun hiring and is well into the process of developing redress procedures that will be refined during the Secure Flight test in November. For present purposes, however, TSA is only testing the Secure Flight concept. Because the data to be used concerns domestic flights that have already been completed during the month of June 2004 – meaning that passengers were already screened – and because the test results will not be used in an operational setting to conduct passenger screening, no passengers will need to avail themselves of the redress process during testing. With respect to special procedures for business travelers, TSA does not, at this point, believe that the Secure Flight program will cause delays that would warrant special treatment for any class of passengers. Information obtained through program testing, however, may be relevant to this issue, and TSA will consider it in developing the operational aspects of the Secure Flight program.

Use of Commercial Data

A number of commenters had questions and concerns regarding TSA's plan to test the use of commercial data to identify passenger information that is incorrect or inaccurate. Commenters expressed concern that TSA's access to commercial information would open the door to abuse of individuals' privacy rights and possible theft of their personal information.

As discussed in detail in the Privacy Impact Assessment for the Secure Flight Test Phase (69 FR 57352), TSA's testing of commercial data will be governed by stringent

data security and privacy protections, including: contractual prohibitions on commercial entities' maintenance or use of PNR information for any purposes other than testing under TSA parameters; strict firewalls between the government and commercial data providers; real-time auditing procedures to determine when data has been accessed and by whom; and strict rules prohibiting the access or use of commercially held personal data by TSA. TSA will not have access to or store the commercially available data that would be used by commercial data aggregators.

One commenter questioned TSA's need for passengers' credit card information as part of Secure Flight and whether TSA would be using commercial data to check credit histories and other personal information unrelated to Secure Flight. Commenters also had questions about the types of commercial information that could lead TSA to apply enhanced screening or deny an individual access to an aircraft. One commenter suggested that TSA use only those sources of commercial data that are easily corrected by consumers so that if there are errors in commercially available data that lead to incorrect screening decisions by TSA, those errors can be resolved in a timely manner.

These are all are key issues that TSA will be attempting to resolve during the testing phase. Once TSA has information about the feasibility and efficacy of using commercial data, such as credit card numbers, to gauge the accuracy of passenger information and reduce false positive matches to information in the TSDB, the agency will be in a position to provide specific answers to the types of questions raised by the commenters. TSA will not have access to individuals' credit histories, medical records, or other personal records.

A number of commenters expressed concern over access by data aggregators to passenger information during the testing. TSA will require the data aggregators with whom it works to abide by the requirements of the Privacy Act as well as to execute legally enforceable nondisclosure agreements prohibiting their use of information for any purpose other than for the testing of the effectiveness of the use of commercial data for Secure Flight. As a security mechanism, TSA has installed an auditing system as part of the platform on which the Secure Flight program will operate. The auditing mechanism will immediately detect any unauthorized access to the passenger data. Within TSA, individuals who are not conducting the test of the Secure Flight program will not have access to any passenger information. The real-time auditing mechanisms in place should prevent unauthorized access by individuals who are not part of the team conducting the test. TSA personnel with access to information for the testing phase will undergo specialized privacy training and will be required to hold appropriate security clearances and, therefore, will understand the sensitivity of the information to which they have access.

Under section 552(d) of the Department of Homeland Security Appropriations Act, 2005 (P.L. 108-334), TSA may not test the use of commercial data until the agency has developed measures to determine the impact of the use of commercial data on aviation security and the Government Accountability Office (GAO) has reported on TSA's evaluation measures. TSA currently is working with GAO to provide the information GAO needs to evaluate TSA's measures.

Efficacy of the Program

Commenters questioned the potential effectiveness of the Secure Flight program because, they claim, the information in the TSDB regarding individuals known or suspected of being engaged in terrorist activity is inaccurate. A number of commenters stated that TSA should instead focus its resources and effort on improved physical security measures such as improved checkpoint screening, increased numbers of Federal Air Marshals and Federal Flight Deck Officers, and improved screening of baggage and cargo. NBTA stated that TSA should stress test the Secure Flight system and develop operational safeguards and oversight policies for the program.

TSA agrees with those commenters who have stated that TSA should ensure that the Secure Flight program is effective before going forward with implementation and should have a quick and effective redress process to address situations in which passengers are mistakenly subjected to enhanced scrutiny or believe that they have wrongly been included on a watchlist.

With respect to the suggested choice between developing Secure Flight or directing TSA's resources towards other security measures, TSA approaches security as a layered process. TSA is committed to taking actions that will improve each layer of security and believes that such actions are not mutually exclusive.

The American Civil Liberties Union (ACLU) commented that the continued expansion of government watchlists creates a risk of false positive matches of passengers on watchlists. Therefore, the ACLU stated, effective management of the watchlists will become even more important. Again, TSA agrees that the Secure Flight program must be

shown to be effective in achieving its stated goals before it is implemented. In order to determine whether the program can be effective, however, TSA must test the system and is doing so while respecting the privacy and civil liberties of individuals.

A number of commenters stated that Secure Flight would not be effective in identifying terrorists who may travel by air but are not currently known to the Federal Government and therefore are not included in the TSDB. Commenters also stated that even if an individual is included in the TSDB, Secure Flight will not detect that individual if he or she assumes the identity of a person not included in the TSDB, such as through identity theft.

TSA agrees that checking passenger names against information in the TSDB will not identify unknown terrorists or those using a stolen identity. Commercial data may be useful in identifying instances where a passenger may have presented inaccurate or incorrect information.

As discussed previously, however, Secure Flight will involve the use of a streamlined version of the existing CAPPS system that aircraft operators currently are using to prescreen passengers. That system evaluates information in PNRs that passengers otherwise provide to aircraft operators in the normal course of business. This element of Secure Flight will address the threat posed by an individual who may pose a threat but is not included in the TSDB or has assumed the identity of a person not included in the TSDB.

A number of commenters stated that TSA should make public the results of the Secure Flight test phase. TSA will make the results available to the extent consistent with national security and homeland security.

Compliance with the Privacy Act, PRA, and Other Laws

The EPIC stated that OMB should not approve the information collection until TSA provides more detailed information to the public about the Secure Flight program.

The Secure Flight program is at a very early stage of development. The purpose of the test phase is to determine the technical feasibility of a consolidated system by which TSA may compare information in PNRs to information in the TSDB. At this point, therefore, TSA has provided as much detail as it can about the planned workings of the Secure Flight program. Once the test is completed and the results are analyzed, if the test phase indicates that the program is technically feasible, TSA will then be able to engage in a public rulemaking process that will involve a more detailed proposal for the Secure Flight program. This subsequent rulemaking will provide members of the public further opportunity to comment on operational and policy issues raised by the program.

One commenter questioned whether TSA had a basis for receiving emergency processing from OMB of the information collection contained in the proposed order. TSA's request for emergency processing was based on the need to move forward with a new passenger prescreening system as quickly as possible, consistent with the 9/11 Commission's recently issued recommendation that TSA take over from aircraft operators the function of passenger prescreening using government watchlists.

The commenter also articulated a number of aspects of the Secure Flight program that he argued are contrary to the requirements of the Privacy Act or other laws. First, he argued that PNRs constitute information regarding an individual's exercise of the First Amendment right of assembly because travel is a form of assembly.

The Privacy Act imposes certain limits on an agency's authority to collect records describing an individual's exercise of First Amendment Rights. See 5 U.S.C. 552a(e)(7). TSA does not agree that PNRs contain information related to the exercise of First Amendment rights, including the right of assembly.

Second, the commenter argued that TSA's proposed order to aircraft operators to submit PNRs is inconsistent with the requirement that an agency collect information to the maximum extent practical directly from an individual when the information may result in an adverse determination about an individual's rights, benefits, or privileges. See 5 U.S.C. 552a(e)(2). The commenter stated that TSA has failed to show that it would be impractical for TSA staff to collect information about passengers from them directly at the airport prior to boarding.

Collecting information from passengers at the airport for purposes of the Secure Flight test would impose a tremendous burden on the flying public in the form of additional time required for security screening. It also would not allow TSA to obtain and test the information in a PNR format, which is the form in which TSA would receive the information during the operational phase of the program.

Third, the commenter, as well as others, stated that the proposed order is inconsistent with the Privacy Act because passengers whose information will be submitted to TSA under the order did not receive notice in accordance with section 552a(e)(3) of the Privacy Act, which requires a Federal agency to "inform each individual whom it asks to supply information" of: (1) the authority under which the request is made; (2) whether the disclosure of the information is mandatory or voluntary; (3) the principal purpose for which the information is intended to be used and the routine

uses which may be made of the information; and (4) the effects on the individual if any, of not providing all or part of the information.

The notice requirement under 5 U.S.C. 552a(e)(3) does not apply to the collection of the PNRs described in the proposed order. OMB has interpreted the notice requirement in section 552a(e)(3) to be inapplicable to situations in which an agency collects information about an individual from a third party.

Fourth, the commenter argues that the system of records notice for Secure Flight fails to meet the requirement in 5 U.S.C. 552a(e)(4)(B) that it describe the categories of individuals on whom records are maintained in the system. The commenter notes that PNRs may contain the names of travel agents or other individuals who make, pay for, or process a passenger's travel but who are not passengers. The commenter also noted that the proposed order covered PNRs with itineraries that were entirely cancelled, thereby capturing individuals who had not flown.

It is our understanding that the inclusion in PNRs of names other than those of passengers is rare. In any case, for purposes of testing the Secure Flight concept, TSA will not retrieve information from PNRs using the names of travel agents or other non-passengers who may be included in a PNR, because the purpose of Secure Flight is to screen passengers. The purpose of listing "Categories of individuals covered" in the system of records notice is to provide notice to those individuals whose records are subject to the Privacy Act because the records are retrieved by their name or personal identifier. The purpose is not to provide notice to every individual whose name may be incidentally mentioned in a record retrieved by the name of another individual. In addition, TSA has revised the final order to exclude from its scope any PNRs with

itineraries that have been cancelled in whole, thereby avoiding collection of PNRs for individuals who have not actually completed any part of the itinerary in the PNR. For these reasons, the provision in the system of records notice meets the requirements of the Privacy Act.

Fifth, the commenter argues that TSA has failed to meet certain requirements applicable to the promulgation of regulations under the Airline Deregulation Act, the Aviation and Transportation Security Act, and the Unfunded Mandates Reform Act of 1995, and the Regulatory Flexibility Act. Other commenters noted that TSA has not published a cost-benefit analysis for the Secure Flight program.

As discussed previously, TSA is obtaining historical PNRs for the test phase of Secure Flight through the issuance of an order, not through rulemaking. Therefore, the foregoing statutes, as well as other statutes and Executive Orders that apply to agency rulemaking, do not apply in this instance. If testing of the program indicates that it is a feasible and effective security measure, TSA will initiate a public rulemaking process in which it will again fully comply with all applicable statutory requirements.

Sixth, the commenter argued that TSA has no authority to establish a system of records for Secure Flight or order aircraft operators to provide PNRs to TSA.

TSA has ample authority conduct the Secure Flight test. Under the Aviation and Transportation Security Act and authority delegated to the Assistant Secretary of Homeland Security (Transportation Security Administration) by the Secretary of Homeland Security, TSA is responsible for, among other things, the screening of passengers and property transported in air transportation and intrastate air transportation. Also under its delegated authority, TSA has broad authority under 49 U.S.C. 40113(a) to

issue orders necessary to carry out its statutory duties, which expressly include providing for security screening, under 49 U.S.C. 44901(a). TSA also is authorized to undertake research and development activities necessary to enhance transportation security under 49 U.S.C. 114(f)(8) and create a successor system to the existing CAPPS under 49 U.S.C. 44903(j)(2). Under these authorities, TSA may order aircraft operators to provide PNRs to TSA to test the Secure Flight program. Implementation of the Secure Flight test also is in furtherance of Homeland Security Presidential Directive-6/HSPD-6 of September 23, 2003 ("Integration and Use of Screening Information to Protect Against Terrorism"), which, among other things, directs Federal agencies to conduct screening at all appropriate opportunities using consolidated terrorist information and intelligence about individuals known or appropriately suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, ore related to terrorism.

Potential Conflict with EU Laws

United Airlines and other commenters expressed concern that complying with the proposed order would expose U.S. airlines to liability for violating privacy laws of the Member States of the EU. United suggested that the U.S. government work closely with foreign governments to address any conflicts of laws that may arise. While TSA has clear statutory authority to require the submission of reservation information for use in prescreening passengers on domestic flight segments, TSA understands the sensitivity of aircraft operators to the possibility of conflicting legal obligations under U.S. law and the laws of EU Member States. Therefore, in the interest of implementing this test expeditiously, TSA has determined that for purposes of this test phase aircraft operators

may opt to exclude from PNRs submitted to TSA any PNR that includes a flight segment between the United States and the EU.

TSA and Department officials briefed European Commission (EC) representatives on October 25 to provide further details on Secure Flight testing, including the parameters of data to be submitted for the test. TSA informed the EC that carriers may elect not to submit to TSA for use in testing any PNRs with a flight segment between the EU and the United States. The Department and EC representatives will continue regular discussions to keep the EU fully apprised of TSA's progress regarding Secure Flight, and to receive EU feedback on Secure Flight issues. TSA, in conjunction with DHS, will continue to consult with the EU prior to and during Secure Flight implementation.

Other Issues

United Airlines stated in its comment the concern that the Secure Flight program might result in unnecessary costs to airlines if they are required to establish new systems to transmit passenger information to TSA, rather than relying on existing systems, such as those that U.S. Customs and Border Protection has in place for receiving advance passenger information for international flights. In planning and developing the operational stage of the Secure Flight program, TSA will work to use existing communications links between the airlines and the Federal Government in order to avoid imposing duplicative requirements on the airlines to the greatest extent possible.

Final Order

The final order is largely unchanged from the proposed order, with the exception of the following provisions.

First, in order to simplify and clarify compliance with the order, TSA changed the scope of PNRs that aircraft operators are required to provide and the description of the category of aircraft operators covered by the order. The proposed order would have required the submission of any PNRs with a flight segment completed during June 2004, so long as all the flight segments in the PNR had been completed by the end of June 2004. Thus, the proposed order covered PNRs with flight segments completed many months before June 2004. The final order applies only to those PNRs with all flight segments (flights between two locations) completed in June 2004.

The proposed order applied to PNRs for any passenger on "a scheduled flight within the United States, in operations subject to a full security program under 49 CFR 1544.101(a)." This language was intended to cover any scheduled passenger or public charter operation conducted under a full security program. Because the proposed order did not specifically mention public charter operations and used the term "scheduled flight," there was some confusion as to whether TSA intended to cover any public charter operations. The final order clarifies this point by stating the following: "This order applies to aircraft operators that conduct scheduled passenger or public charter operations subject to a full security program under 49 CFR 1544.101(a)."

The proposed order directed aircraft operators to exclude from the PNRs submitted to TSA any flight segment to or from the United States. TSA now understands, however, that deleting information related to flight segments from PNRs is difficult and could inhibit aircraft operators from complying with the order in a timely manner. After reviewing this issue and considering the issues discussed above related to possible conflicts of law with EU Member States, TSA

revised the order to allow aircraft operators to exclude entirely from its submission PNRs that include flight segments between the United States and the EU.

TSA has modified the proposed order in response to questions about how the order applied to aircraft operators that use passenger manifests rather than PNRs. The final order provides that if an aircraft operator does not use PNRs, the order applies to the reservation data in whatever form the aircraft operators receive or maintain for operation of a flight, such as a passenger manifest. The final order also clarifies that with respect to codesharing operations, if an aircraft operator does not maintain PNRs or other passenger reservation information for the flights that it operates, the aircraft operator may comply with the order by stipulating in writing to TSA that the entity maintaining such PNRs or other passenger reservation information has agreed to provide the information to TSA on behalf of the aircraft operator. For example, a regional aircraft operator that relies on other aircraft operators to maintain PNRs for the regional operator's flights must stipulate that the other aircraft operators will submit PNRs to TSA on the regional aircraft operator's behalf.

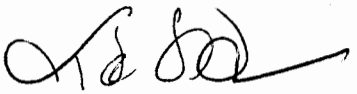
TSA also received questions about how to address situations where PNR history, which was excluded from the scope of the proposed order, includes completed flight segments, which were included in the scope of the proposed order. The final order clarifies that if the PNR history includes information on flight segments already flown, they must be included in the PNR submitted to TSA. In such cases, the aircraft operator may move information on flights flown

out of the PNR history or include the entire PNR history in the information submitted to TSA, and TSA will extract the flown flight segments. The final order also clarifies that PNRs must include all data that would have been available to the aircraft operator prior to the completion of the itinerary (active fields), including any "remarks" sections, the reservation creation date, and CAPPS scores and codes.

Finally, the final order provides additional information about how the PNRs are to be submitted, including a requirement that they be password protected.

Based on the foregoing, TSA will issue the following final order to aircraft operators. The text of the final order is set forth below.

Issued in Arlington, Virginia, on NOV 1 0 2004



Lisa S. Dean,

Privacy Officer.

"OMB Control Number 1652-0025
Expiration Date: March 31, 2005

TRANSPORTATION SECURITY ADMINISTRATION
ORDER

Pursuant to the authority vested in me as Assistant Secretary of Homeland Security (Transportation Security Administration) (TSA) by delegation from the Secretary of Homeland Security, 49 U.S.C. 40113(a), and other authorities described below, I hereby direct each aircraft operator listed in Attachment A to this order to provide passenger name records (PNRs) to TSA in accordance with the terms of this order.

Background and Authority

1. The Secretary of Homeland Security has delegated to the Assistant Secretary of Homeland Security (TSA), subject to the Secretary's guidance and control, the authority vested in the Secretary by section 403(2) of the Homeland Security Act respecting TSA, including that related to civil aviation security under the Aviation and Transportation Security Act.

2. Under 49 U.S.C. 114(e)(1) and 44901(a), TSA is responsible for, among other things, providing for the screening of passengers traveling in air transportation and intrastate air transportation.

3. One component of passenger screening is the Computer-Assisted Passenger Prescreening System (CAPPS), an automated screening system developed by the Federal Aviation Administration (FAA) in cooperation with U.S. aircraft operators. U.S. aircraft operators implemented CAPPS in 1997.

4. CAPPS evaluates information in PNRs that passengers otherwise provide to aircraft operators in the normal course of business to determine whether a passenger will be selected for a higher level of security screening prior to boarding. A PNR is a record that contains detailed information about an individual's travel on a particular flight, including information provided by the individual when making the flight reservation. While the Federal Government established the CAPPS selection criteria, CAPPS is operated entirely by U.S. aircraft operators.

5. Passenger prescreening also involves the comparison of identifying information of airline passengers against lists of individuals known to pose or suspected of posing a threat to civil aviation or national security. Aircraft operators currently carry out this function, using lists provided by TSA. Because the lists are provided in an unclassified form, the amount of information they include is limited. For this reason, TSA will take over from aircraft operators the function of screening passengers against such lists and use a larger set of data maintained by the Federal Government for this purpose. This is consistent with the recommendation by the National Commission on Terrorist Attacks upon the United States (9/11 Commission) related to the use of expanded "No-Fly" and "Automatic Selectee" lists, and the 9/11 Commission recommendation that aircraft operators be required to supply the information needed to test and implement such a system.

6. In accordance with the authority in 49 U.S.C. 44903(j)(2), TSA is in the process of developing a successor system to CAPPS that will be

operated entirely by TSA and will incorporate the screening of passengers against data maintained by the Terrorist Screening Center (TSC) about individuals known or reasonably suspected to be or have been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism.

7. In order to test such a system, TSA must have access to information contained in the PNRs for domestic passenger flights. TSA also must have access to passenger information from aircraft operators that maintain the information in forms other than PNRs, such as passenger manifests.

8. TSA has broad authority under 49 U.S.C. 40113(a) to issue orders necessary to carry out its functions, including its responsibility to provide for the security screening of passengers under 49 U.S.C. 44901(a). TSA also has authority to identify and undertake research and development activities necessary to enhance transportation security under 49 U.S.C. 114(f)(8).

Findings

9. The security prescreening of passengers, as mandated by Congress, is vital to aviation security and national security.

10. After a lengthy review of the initial plans for a successor system to CAPPS, and consistent with the recommendation of the 9/11 Commission, the Department of Homeland Security is moving forward with a next generation system of domestic passenger prescreening that meets the following goals: (1) identifying, in advance of flight, passengers known or suspected to be engaged in terrorist activity; (2) moving of passengers through airport screening more quickly and reducing the number of individuals unnecessarily selected for secondary screening; and (3) fully protecting passengers' privacy and civil liberties.

11. In the revised program, known as Secure Flight, TSA will compare information in airline PNRs or other passenger manifest formats for domestic flights to information in the Terrorist Screening Database (TSDB) maintained by TSC, including expanded TSA No-Fly and Selectee lists, in order to identify individuals known or reasonably suspected to be or having been engaged in conduct constituting, in preparation for, in aid of, or related to terrorism. The Secure Flight program also will test operation of a streamlined version of the existing CAPPS evaluation criteria. TSA will use the PNRs obtained under this order to test these aspects of the program.

12. TSA also will test whether comparing passenger information to other commercially available data can enhance TSA's ability to identify passenger information that is inaccurate or incorrect.

13. In order to develop and test such a system, TSA must obtain passenger information in PNRs, or other passenger manifest formats where PNRs are not used, from aircraft operators.

14. On September 24, 2004, TSA published in the Federal Register a proposed order requiring aircraft operators to provide PNRs for testing the Secure Flight program. After considering the public comments received and making modifications to the proposed order, where appropriate, TSA is issuing this final order to aircraft operators for purposes of obtaining PNRs to test the Secure Flight program.

Action Ordered

15. Scope:

a. Aircraft Operators:

This order applies to aircraft operators that conduct scheduled passenger or public charter operations subject to a full security program under 49 CFR 1544.101(a).

b. Information:

This order applies to PNRs containing itineraries for domestic flights operated under a full security program and for which all flight segments in the itinerary were flown between June 1, 2004 and June 30, 2004, (after 2400 hours 31 May 2004 and before 0001 hours 1 July 2004). This includes PNRs for non-revenue and space available passengers.

For purposes of this order, "PNR" means the electronic record maintained by the aircraft operator detailing information about an individual's travel on a particular flight and any other information contained in that record.

For purposes of this order, "domestic flight" means a flight between two locations in the United States (to include the U.S. Virgin Islands, Puerto Rico, Guam, Saipan, and American Samoa).

This order does not apply to PNRs reflecting itineraries that were cancelled in whole.

An aircraft operator may elect to exclude from the scope of the order any PNRs which include any flight segments between the EU and the United States.

If an aircraft operator does not use PNRs, the order applies to the reservation data in whatever form aircraft operators receive or maintain for operation of a flight, such as a passenger manifest.

c. Information in PNRs:

PNRs must include all data that would have been available to the aircraft operator in a displayed PNR prior to the completion of the itinerary (active fields), including any "remarks" sections, the reservation creation date, and CAPPS scores and codes.

PNRs may not include information related to changes in a PNR prior to completion of the flight itinerary (PNR history). If, however, the PNR history includes information on flight segments already flown, they must be included in the PNR. In such cases, the aircraft operator may move information on flights flown out of the PNR history or include the entire PNR history in the information submitted to TSA, and TSA will extract the flown flights segments (itinerary).

PNRs may be submitted in archive format.

16. Submission of PNRs:

The aircraft operator must submit to TSA all PNRs described in paragraph 15 so that the data is received by TSA no later than 5:00 p.m. EST on November 23, 2004.

Mail all information through overnight carrier to:
Lisa Dean, Privacy Officer
Transportation Security Administration
601 S. 12th Street, TSA-9, Room E7-305N
Arlington, VA 22202
Phone: 571-227-3947

17. Codesharing Operations:

If an aircraft operator does not maintain PNRs or other passenger reservation information for the flights that it operates, the aircraft operator may comply with this order by stipulating in writing to TSA that the entity maintaining such PNRs or other passenger reservation information has agreed to provide the information to TSA on behalf of

the aircraft operator. For example, a regional aircraft operator that relies on other aircraft operators to maintain PNRs for the regional operator's flights must stipulate the other aircraft operators will submit PNRs to TSA on the regional aircraft operator's behalf.

Letters of stipulation, described above, must be signed and on company letterhead. They may be delivered in one of the following three ways:

US Mail:
TSA/ONRA
Attention: Airline Team
P.O. Box 597
Annapolis Junction, MD 20701

FAX: 240-568-3528

E-mail (scanned copies): SecureFlight@DHS.gov

18. The aircraft operator must provide to TSA information about the aircraft operator's PNR data schema and layout, such as a PNR format book and a data dictionary that includes all acronyms and codes not standard to the International Air Transport Association.

19. For purposes of the test, the aircraft operator must provide the PNRs to TSA on optical media in an unpacked or uncompressed form, in a structured data format or XML, if available. Information must be password-protected. The aircraft operator must supply TSA with the password via e-mail at SecureFlight@DHS.gov.

ATTACHMENT A—AIRCRAFT OPERATORS

1. Air Midwest Inc.
2. Air Wisconsin Airline Corp
3. AirTran Airways Inc.
4. Alaska Airlines Inc.
5. Allegiant Air
6. Aloha Airlines Inc.
7. America West Airlines Inc.
8. American Airlines Inc.
9. American Eagle
10. American Trans Air Inc.
11. Atlantic Southeast Airlines (ASA)
37. Hawaiian Airlines
38. Horizon Air
39. Independence Air (Atlantic Coast Airline)
40. Jetblue Airways Corp.
41. Kenmore (start-up)
42. Mesa Airlines
43. Mesaba Aviation Inc.
44. Miami Air International
45. Midwest Airlines Inc.
46. North American Airlines
47. Northwest Airlines Inc.

12. Big Sky Airlines
13. Boston and Maine Airways
14. Cape Air (Hyannis Air Service)
15. Caribbean Air
16. Casino Airlines

17. Casino Express TEM Enterprises
18. Champion Air (Grand Holdings)
19. Chautauqua Airlines
20. Chicago Express Airlines

21. Colgan Air
22. Comair, Inc.
23. Commutair (Champlain Ent.)
24. Continental Airlines Inc.
25. Continental Micronesia Inc.
26. Corporate Airlines

27. Delta Air Lines Inc.
28. Executive Airlines/American Eagle

29. Expressjet Airlines (Cont. Express)

30. Falcon Air Express
31. Freedom Air
32. Freedom Airlines
33. Frontier Airlines
34. Great Lakes Aviation Ltd..
35. Gulfstream International Airlines
36. Hawaii Island Air (Island Air)

48. Omni
49. Pace/Hooters
50. Pacific Island Aviation Inc.

51. Pacific Wings
52. Pan American Airways Corp.
53. Piedmont Airlines

54. Pinnacle Airlines (d/b/a Northwest Airlink)
55. Planet Air
56. Primaris Airlines, Inc. (Primaris)
57. PSA Airlines
58. Ryan International Airlines
59. Shuttle America
60. Sky King
61. Sky West Airlines
62. Skyway Airlines/Midwest Connect
63. Southeast Airlines
64. Southwest Airlines (U.S.A.)

65. Spirit Airlines

66. Sun Country Airlines Inc.
67. Trans States Airlines
68. Transmeridian Airlines
69. United Airlines Inc.
70. US Airways Inc
71. USA3000

72. World Airways"